Florida Law Review

Volume 60
Issue 5 *December 2008*

Article 6

11-18-2012

Possession of Child Pornography: Should You be Convicted When the Computer Cache Does the Saving for You?

Giannina Marin

POSSESSION OF CHILD PORNOGRAPHY: SHOULD YOU BE CONVICTED WHEN THE COMPUTER CACHE DOES THE SAVING FOR YOU?

Giannina Marin[*]

---

* To my parents, Javier and Eva, my sister Natalia, and my husband Larry. Thank you for your unwavering support.

I. INTRODUCTION

"*For years, defense lawyers have argued the 'young and stupid' semi-defense for their youthful clients. Now, we can have the 'I didn't know it was on the hard drive' objection for the unsophisticated computer user in child pornography cases—or at least they can in the 9th Circuit.*"[1]

This quote, appearing on the website of an East Texas criminal defense law firm, refers to the outcome of *United States v. Kuchinski*.[2] In *Kuchinski*, the defendant's computer contained, in various forms, more than 15,000 images of child pornography.[3] There was no question that Kuchinski's volitional viewing of the images on the Internet was the sources of those images.[4] No one argued that Kuchinski did not have control over his computer while he searched for the 15,000 images or while he looked at them on his computer screen.[5] However, Kuchinski successfully argued that he lacked knowledge of a computer mechanism that automatically downloads any images viewed while a user surfs the Internet.[6] Ultimately, Kuchinski was convicted for possession of only 110 of the 15,000 images.[7]

The result of *Kuchinski* is a new defense for willing users of child pornography: lack of knowledge regarding the inner workings of their computers,[8] even though a user does not need any advanced computer knowledge to search, view, and control web images.[9] These volitional searches for child pornography provide a user with access to and control over child pornography images.[10] Courts have struggled with such facts,[11]

---

1. F.R. Files, Jr., *The "I Didn't Know It Was on My Hard Drive" Objection*, THE FED. CORNER, Jan.–Feb. 2007, http://bainfiles.com/CM/Articles/The-Federal-Corner-January-February-2007.asp (last visited Sept. 10, 2008).

2. 469 F.3d 853 (9th Cir. 2006).

3. *Id.* at 856.

4. *See id.* at 862 (noting Kuchinski never argued that he did not access the images from the Internet).

5. *See id.* (noting that Kuchinski never argued a lack of control over his computer). In fact, Kuchinski had full ability to control and manipulate the images as he searched for them and held them on his computer screen; *see infra* text accompanying notes 61–63.

6. *Kuchinski*, 469 F.3d at 861–62. For an explanation of the intricacies of the process, see *infra* text accompanying notes 60–75.

7. *Kuchinski*, 469 F.3d at 861–62.

8. *See* Files, *supra* note 1.

9. *See infra* notes 61–66 and accompanying text.

10. *Id.*

11. *See infra* Part IV.

questioning whether it is sound public policy to allow the user to escape liability for possession of child pornography because the user remains ignorant about computers.

This problem is easily identified but much less easily eliminated. The concept of "possession" seems intuitive when one thinks of a physical object: holding something, touching it, feeling it, having it physically present.[12] Therefore, mere viewing, even window-shopping, does not constitute possession of what is on the other side of the glass because one cannot hold it, touch it, or feel it. Even though the legal definition of possession sets forth constraints that limit this basic idea, the general intuition behind possessing an item does not change.[13] In contrast, the concept of possessing something digital is more elusive. Looking at materials on a computer screen might seem more like window-shopping than physical interaction with the materials. However, surfing the Internet involves significant interaction and exchange of information between a user's computer and the web servers visited.[14] Furthermore, the user retains a significant level of control over the information on the computer.[15]

This Note examines the concept of electronic possession in the field of child pornography, with the aim of reconciling the basic intuition behind possession with the reality of electronic data.[16] Part II briefly discusses the case and statutory history that placed child pornography outside the bounds of the First Amendment and led to constitutionally valid prohibitions on the possession of child pornography. Part III sets forth the various ways in which individuals can access electronic child pornography, with a focus on the user's level of interaction. Part IV discusses factors that the courts have considered in defining what constitutes possession of electronic child pornography and critically analyzes two leading court opinions. Part V suggests a test that can be uniformly applied to any situation giving rise to possession of child pornography and discusses how the analysis of previous cases might have been different under the proposed test.

---

12. Webster's Dictionary defines possession, amongst others, as "actual physical control." WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE 1770 (1993).

13. Black's Law Dictionary defines possession as "[t]he fact of having or holding property in one's power; the exercise of dominion over property." BLACK'S LAW DICTIONARY 1201 (8th ed. 2004). Constructive possession is defined as "[c]ontrol or dominion over a property without actual possession or custody of it." *Id.*

14. *See infra* Part III.

15. *See id.*

16. This Note assumes that the court has separately determined whether the material constitutes child pornography and will not discuss the factors considered in that determination.

II. REGULATION OF CHILD PORNOGRAPHY

As early as the 1800s, Congress addressed the legality of obscene materials, a subset of which is child pornography.[17] In *Roth v. United States*,[18] the Supreme Court declared that "obscenity is not within the area of constitutionally protected speech."[19] In 1969, the Supreme Court struck down a Georgia statute that criminalized the possession of obscene materials.[20] Though reasserting its prior position that the First Amendment does not protect obscenity, the Court held that "[i]f the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch."[21]

In the next decade, Congress enacted the Protection of Children Against Sexual Exploitation Act of 1977, which banned *obscene* child pornography.[22] At this time, it was possible for materials involving child pornography to be deemed not obscene; therefore these prosecutions required proof of obscenity.[23] In *New York v. Ferber*,[24] the Supreme Court

---

17. *See* Swearingen v. United States, 161 U.S. 446, 449–50 (1896) (reviewing a charge against defendant for mailing an article that was described to be "obscene, lewd, and lascivious"). In 1948, Congress enacted 18 U.S.C. § 1461 into the Criminal Code, prohibiting the mailing of obscene, lewd, or lascivious materials. 18 U.S.C. § 1461 (current version at 18 U.S.C. § 1461 (2006)); Hamling v. United States, 418 U.S. 87, 91 (1974). Prosecutions related to child pornography proceeded under § 1461. *See infra* note 22 (discussing the prosecution of possession of child pornography under obscenity statutes).

18. 354 U.S. 476 (1957).

19. *Id.* at 485; *see also* § 1461 (prohibiting the mailing of obscene, lewd or lascivious materials).

20. Stanley v. Georgia, 394 U.S. 557, 559 (1969).

21. *Id.* at 565. *Compare id. with Roth*, 354 U.S. at 483 (commenting that at the time of the First Amendment's adoption, obscenity was outside the protection intended for speech and press).

22. *See* Protection of Children Against Sexual Exploitation Act of 1977, Pub. L. No. 95-225, § 2251, 92 Stat. 7 (1978). Until 1977, child pornography offenses were prosecuted only under obscenity statutes, and some prosecutions proceeded under § 1461 even after the enactment of § 2251. *See* United States v. Kussmaul, 987 F.2d 345, 347 n.1 (6th Cir. 1993) (prosecuting under § 1461).

23. United States v. Langford, 688 F.2d 1088, 1092 (7th Cir. 1982) ("[C]hild pornography like other sexually explicit material had to be determined obscene."). In determining whether child pornography was obscene, the Court applied the obscenity test articulated in *Miller v. California*. *Id.* at 1093 (citing Miller v. California, 413 U.S. 15 (1973)). The *Miller* test asked:

> (a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken

upheld a New York statute[25] that banned the dissemination of child pornography without requiring proof that the images were obscene.[26] In upholding New York's ban on child pornography distribution, the Supreme Court focused on the long-lasting detrimental effects on the children involved and rejected the defendant's contention that states should only be allowed to ban obscene materials generally.[27]

In the years following *New York v. Ferber*, states continued to prosecute distribution of child pornography.[28] The result was that the child pornography dissemination moved to an underground market, and, in an effort to decrease demand and production, the states responded by proscribing possession of child pornography.[29] In 1989, the Supreme Court reviewed a challenge to an Ohio statute that proscribed both the possession and the viewing of child pornography.[30] The Court upheld the statute.[31] First, the Court identified the state's interest in protecting the underage victims of child pornography.[32] It distinguished that strong interest from the "weak" concern for the effects of obscene materials on the mind of the viewer—a concern it had rejected in *Stanley v. Georgia*.[33] The Court thus allowed the state to ban possession as a means of controlling child abuse caused by the production and distribution of child pornography.[34] Bans on the mere possession of child pornography thereby became valid.

Federal child pornography statutes currently are codified at 18 U.S.C. §§ 2251–2260 (2006). Specifically, possession of child pornography is banned by § 2252[35] and § 2252A[36] (Child Pornography Prevention Act of 1996).[37] Many states also prohibit possession of child pornography.[38] The

---

as a whole, lacks serious literary, artistic, political or scientific value.

Miller, 413 U.S. at 24 (internal citations omitted).

24. 458 U.S. 747 (1982).

25. N.Y. PENAL LAW § 263.15 (McKinney 1977) (current version at N.Y. PENAL LAW § 263.15 (McKinney 2008)).

26. *Ferber*, 458 U.S. at 778.

27. *Id.* at 760–61 (stating that because the strong interest involved was protecting the children used to make child pornography, the obscene quality of the matter "[bore] no connection to the issue").

28. *See, e.g.*, Osborne v. Ohio, 495 U.S. 103, 109 n.4 (1990).

29. *Id.* at 110–11.

30. *See id.* at 111; *see also* OHIO REV. CODE ANN. § 2907.323(A)(3) (West 2008).

31. *Osborne*, 495 U.S. at 111.

32. *Id.* at 109.

33. *Id.* at 109–10 (citing Stanley v. Georgia, 394 U.S. 557, 567–68 (1969)); *see supra* text accompanying notes 20–21.

34. *See Osborne*, 495 U.S. at 111.

35. Child Protection Act of 1984, 18 U.S.C. § 2252 (2006).

36. Child Pornography Prevention Act of 1996, 18 U.S.C. § 2252(a) (2006).

37. *See also* Henry Cohen, *Child Pornography: Constitutional Principles and Federal*

language of the various statutes is quite similar.[39] Importantly, the Federal statute and various state statutes proscribe only *knowing* possession.[40] The similarities have allowed courts applying the statutes to look beyond their jurisdictions for authority on what constitutes possession of child pornography.[41]

III. ACCESSING CHILD PORNOGRAPHY[42]

A. *Searching for Child Pornography*

Child pornography may be found by searching the Internet.[43] The names of child pornography files, like many other computer files, commonly reference their content.[44] Common child pornography-related Internet search terms include "illegal[,] preteen[,] underage[,] lolita[,]

Statutes, *in* GOVERNMENTAL PRINCIPLES AND STATUTES ON CHILD PORNOGRAPHY 1, 7, 10 (Walker T. Holliday ed., 2003). Sections 2252 and 2252A operate independently to proscribe *knowing* possession in similar, although not identical, words. *Compare* 18 U.S.C. § 2252(a)(4)(B)(i-ii) (applying to child pornography depicting actual children), *with* 18 U.S.C. § 2252A(a)(5)(B) (applying to child pornography that is also computer-generated), *and* 18 U.S.C. § 2256 (defining "visual depiction" and "child pornography").

38. *See, e.g.*, ALA. CODE § 13A-12-192(b) (2008) ("Any person who *knowingly* possesses . . . shall be guilty . . . ." (emphasis added)); ARIZ. REV. STAT. ANN. § 13-3553(A)(2) (2008) ("A person commits sexual exploitation of a minor by *knowingly* . . . possessing . . . ." (emphasis added)); FLA. STAT. § 827.071(5) (2008) ("It is unlawful for any person to *knowingly* possess . . . ." (emphasis added)); TENN. CODE ANN. § 39-17-1003(a)(1)–(2) (2008) ("It is unlawful for any person to *knowingly* possess . . . ." (emphasis added)).

39. *See supra* note 38 and accompanying text.

40. *See supra* notes 37–38 and accompanying text.

41. *See* United States v. Romm, 455 F.3d 990, 998 (9th Cir. 2006) (citing United States v. Tucker (*Tucker II*), 305 F.3d 1193, 1204 (10th Cir. 2002)); *see also* Strouse v. State, 932 So. 2d 326, 329 (Fla. 4th DCA 2006) (citing United States v. Perez, 247 F. Supp. 2d 459, 484 n.12 (S.D.N.Y. 2003)). Arguably, the creation of the Internet has allowed for the dissemination of child pornography on a new and larger scale, thus forcing courts to examine existing analyses and apply them to new scenarios. *See* Jessica McCausland, Note, *Regulating Computer Crime After Reno v. ACLU: The Myth of Additional Regulation*, 49 FLA. L. REV. 483, 491 (1997) (noting that "[despite all the concern, some courts have had little trouble applying established concepts to the new factual situations presented by the internet").

42. For purposes of this Note, "to access an image" means viewing it on a computer without necessarily having intentionally saved a copy of the image onto the computer. *See, e.g.*, Commonwealth v. Diodoro, 932 A.2d 172, 174 (Pa. Super. Ct. 2007). "Downloading" will refer to the intentional act by the user to create a copy of the image on his hard drive. *See, e.g.*, United States v. Riccardi, 258 F. Supp. 2d 1212, 1224 (D. Kan. 2003).

43. State v. Morris, No. 04CA0036, 2005 WL 356801, at *1 (Ohio Ct. App. Feb. 16, 2005) (noting that witnesses discussed searches that are used to arrive at web site images of child pornography).

44. *See* MAX TAYLOR & ETHEL QUAYLE, CHILD PORNOGRAPHY: AN INTERNET CRIME 162 (2003) (discussing identifiers).

kiddy[,] child[, and] incest[.]"[45] These terms specifically refer to child pornography and differ from terms associated with adult pornography.[46] As such, a user seeking child pornography can direct a search to specifically yield child pornography. However, it is possible for a child pornography image to be mislabeled.[47] Therefore, a user seeking to download only adult pornography, who did not input any child-related search terms, could inadvertently find child pornography.

B. *Downloading Images*

The Internet provides multiple avenues to access child pornography. The methods can be categorized as those that involve the viewing of child pornography off an Internet server versus those that involve downloading the image to the user's computer.[48] As the term is generally used, downloading an image requires a positive effort by the viewer to make a copy of the image in his hard drive.[49] The person must instruct the computer to save or download the image and designate where it should store the image.[50] Case law reveals that child pornography consumers use a wide variety of methods to download images.[51] Users can use a web browser to download images directly off the websites.[52] File sharing programs such as Kazaa and BearShare allow users to share files by downloading them from another user's computer.[53] Images can also be

---

45. *Morris*, 2005 WL 356801, at *5. "'Lolita' is often a code word for child pornography." United States v. Grimes, 244 F.3d 375, 379 n.7 (5th Cir. 2001).

46. *See Morris*, 2005 WL 356801, at *5 ("[T]hese search terms were commonly used in attempts to locate child pornography on the Internet.").

47. *See* U.S. GEN. ACCOUNTING OFFICE, FILE SHARING PROGRAMS: USERS OF PEER-TO-PEER NETWORKS CAN READILY ACCESS CHILD PORNOGRAPHY 11 (2004), *available at* http://www.gao.gov/new.items/d04757t.pdf [hereinafter GAO REPORT] (discussing "innocuous searches" that may lead to child pornography).

48. *See* Commonwealth v. Diodoro, 932 A.2d 172, 174 (Pa. Super. Ct. 2007) (addressing defendant's claim that he did not download images to his computer, rather he solely viewed the images online).

49. United States v. Riccardi, 258 F. Supp. 2d 1212, 1224 (D. Kan. 2003).

50. *Id.*

51. *See* United States v. Griffin, 482 F.3d 1008, 1010 (8th Cir. 2007) (addressing the utilization of Kazaa, a file-sharing network); *Riccardi*, 258 F. Supp. 2d at 1224 (considering the utilization of AOL).

52. *See, e.g.*, United States v. Carani, 492 F.3d 867, 871 (7th Cir. 2007) (stating two of the files were "accessed through a web browser").

53. GAO REPORT, *supra* note 47, at 17. Simply put, these programs provide a meeting place where the users can search the files of others and download them. *Id.* at 16–17. The user prompts both the search and the download. *See id*.; *see also Carani*, 492 F.3d at 869. The program searches, then returns a list of available matches for the user's criteria and provides the user with information about the files. *Id.*

transferred between computer users through Internet chat groups[54] or newsgroups.[55] Finally, images can be obtained, copied, or transferred by the use of removable storage such as CDs, floppy disks, or flash drives.[56]

Once saved to the computer's hard drive, the saved image becomes part of the data on the computer and can be accessed at any time without an Internet connection.[57] At this point, the user controls the image's destiny: The user can enlarge it, zoom in, zoom out, rotate it, print it, share it, edit it, and delete it.[58] In fact, even if the user decides not to look at an image ever again, the image will remain on the computer until the user takes affirmative steps to delete it.[59]

C. *Viewing Images on the Internet Without Downloading and the Problematic Side-Effect: Cache Memory*

The user may choose to view the images on the Internet without downloading them onto the hard drive.[60] Websites featuring child pornography include thumbnails that the viewer can enlarge.[61] While the image is on the viewer's screen, the user is in control of the image.[62] The viewer can undertake largely the same actions as if the image had been downloaded: He can enlarge it, zoom in or out, rotate it, print it, copy it to his computer, and show it to others.[63] Nevertheless, at this point, despite the user's apparent control over the image, the average defendant will still argue that he does not possess child pornography.[64]

---

54. GAO REPORT, *supra* note 47, at 1.

55. *See* TAYLOR & QUAYLE, *supra* note 44, at 166. Newsgroups are classified by interests. *See id*. The user can seek out the appropriate group through which to access child pornography. *See id.*

56. *See* United States v. White, 506 F.3d 635, 638 (8th Cir. 2007) (noting that defendant copied images of child pornography onto disks, which he labeled and stored).

57. *See, e.g.*, United States v. Riccardi, 258 F. Supp. 2d 1212, 1224 (D. Kan. 2003) (addressing a situation in which a user "unzipped" files to save them on his computer).

58. *See* TAYLOR & QUAYLE, *supra* note 44, at 85 ("One function of the Internet in relation to this was that images could be downloaded and changed, to meet the needs of the collector . . . ."); *see also* United States v. Tucker (*Tucker I*), 150 F. Supp. 2d 1263, 1267 (D. Utah 2001) (discussing the ways in which a user can control the image).

59. *See, e.g.*, *Tucker I*, 150 F. Supp. 2d at 1265 (noting the affirmative steps taken to delete images).

60. *See, e.g.*, *id.* (addressing a situation in which pornographic pictures were stored on the defendant's computer cache file).

61. *See id.*

62. *See id.* at 1267.

63. *Id.*; *see supra* note 58 and accompanying text.

64. Defendants often argue that mere viewing of child pornography online, without downloading, does not constitute possession of child pornography. *See, e.g.*, United States v. Romm, 455 F.3d 990, 993–94 (9th Cir. 2006); United States v. Tucker (*Tucker II*), 305 F.3d 1193, 1204 (10th Cir. 2002); United States v. Bunnell, No. CRIM. 02-13-B-S, 2002 WL 927765, at *1

However, to speed up repeat viewing of a previously visited website, computers automatically make a copy of the data from visited websites in the form of "temporary Internet files" and store the data in what is called the "cache."[65] Therefore, the first time a user visits a website two simultaneous processes occur: (1) the computer opens the website and shows it on the screen, and (2) the computer creates a copy of all the data on that website and stores it in the cache.[66] When the user revisits the website, the computer compares the date on the website to the date on the previously stored temporary file; if unchanged, the computer displays the cached file on the screen, but, if the website has been updated, the computer displays the data from the website.[67]

This process occurs automatically, without any prompting by the user, any time an Internet user visits any website; thus, it is generally outside the control of Internet users.[68] In fact, since there is no indication to the user that this process is occurring, a computer user could take full advantage of the Internet-surfing capabilities of his computer without ever learning what is happening behind the scenes.[69] Although it is possible to deactivate the cache function of a computer, the average computer user does not know how or why the process works.[70] Even users that have a general idea of the

---

(D. Me. May 10, 2002); Ward v. State, No. CR-05-1277, 2007 WL 1228169, at *2 (Ala. Crim. App. Apr. 27, 2007); Commonwealth v. Diodoro, 932 A.2d 172, 174 (Pa. Super. Ct. 2007); State v. Pickett, No. M2004-00732-CCA-R3-CD, 2005 WL 2438385, at *6 (Tenn. Crim. App. Oct. 3, 2005).

65. *Ward*, 2007 WL 1228169, at *9.

66. Crucially, these processes are simultaneous, but separate. The image on the computer screen remains on the screen by virtue of the random-access memory (RAM), the memory that operates when files or programs are running. However, despite being identical to the image that was on the screen, the image in the cache is just a copy of that other image and is thus a completely different image. *See Tucker I*, 150 F. Supp. 2d at 1265 n.2 (discussing the functioning of a computer's cache).

67. *See* JIM HANDY, THE CACHE MEMORY BOOK 9 (2d ed. 1998). Court opinions and scholarly articles do not usually discuss this fact. Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227, 1249 (2004). A possible reason is that the average defendant does not seem to be visiting the same images more than once, thus making it irrelevant. *See, e.g.*, *Tucker I*, 150 F. Supp. 2d at 1265 (noting a defendant's statement that new images are always available). At the same time, depending on the approach taken to determine possession, this fact could complicate the analysis of the element of knowledge. *See* Howard *supra* at 1240–43 (discussing the difficulties of proving the element of knowledge where the defendant argues a lack of knowledge as to the workings of the cache).

68. *See* Commonwealth v. Simone, No. CRIM. 03-0986, 2003 WL 22994238, at *3 (Va. Cir. Ct. Nov. 12, 2003), *rev'd*, No. 0551-04-1, 2005 WL 588257, at *4 (Va. Ct. App. Mar. 15, 2005) (reversing conviction because the user "did not have sufficient dominion and control over the computer on [the date alleged in the indictment]").

69. *See id.* ("[T]here is no mechanism on the computer screen that notifies a user . . . .").

70. *See id.*

process's function and operation might not know how to prevent it.[71] A user needs advanced computer skills to directly access files in the cache while the computer is offline.[72] Once properly accessed from inside the computer, however, temporary files are, for all relevant purposes, real files that contain images that can be managed and manipulated like any other file, independent of an Internet connection.[73] Finally, the cache can be easily deleted through the web browser without any special knowledge,[74] or it can be deleted as part of routine computer maintenance.[75]

D. *Somewhere in the Middle: E-mail as a Source*

Images of child pornography can be sent as attachments to e-mail.[76] Viewers can solicit these e-mails by subscribing to chat rooms or websites that send e-mails to their subscribers.[77] It is also possible for Internet users to receive unsolicited e-mails containing child pornography. Depending on the program that the computer operator uses to access e-mails, the attachment , like the cache, might be automatically downloaded onto the computer or can instead be held by a remote server from which the user can manually download or access it at any time. Either way, the user can choose to keep or delete any solicited or unsolicited e-mails he receives. He can therefore willingly choose what e-mails and attachments he keeps, even if he could not control the receipt of the e-mails.

IV. THE COURTS' APPROACH TO POSSESSION

A. *Overview of Factors Considered by the Courts*

Courts' approaches to determining whether a defendant possessed child pornography have lacked uniformity and consistency. Because courts

---

71. *See* United States v. Kuchinski, 469 F.3d 853, 862 (9th Cir. 2006).

72. *See id.* Accessing the cache requires the user to know its location and to override system warnings. United States v. Romm, 455 F.3d 990, 998 (9th Cir. 2006).

73. *Compare* United States v. Tucker (*Tucker II*), 305 F.3d 1193, 1204–05 (10th Cir. 2002) ("Anything [a user] could do with any other file he could do with [the pornographic] files."), *with supra* text accompanying note 58 (discussing the scope of control a user has in manipulating images).

74. Web browsers offer an option to clean that cache with a few simple clicks. In Internet Explorer, for example, it is located in the "General" tab of the "Internet Options" menu which is in turn located under the "Tools" menu. In Firefox, the user can click "Tools" and then "Clear Private Data" in order to clear the cache.

75. *Romm*, 455 F.3d at 995. Specifically, when the cache becomes full, the files in the cache are deleted one by one, with the oldest one being deleted first. HANDY, *supra* note 67, at 9.

76. *See* Fabiano v. Armstrong, 141 P.3d 907, 908 (Colo. Ct. App. 2006) (noting a user's receipt of child pornography images via e-mail).

77. *See* United States v. Perez, 247 F. Supp. 2d 459, 465 (S.D.N.Y. 2003); *Fabiano*, 141 P.3d at 908.

consider different factors,[78] they often reach inconsistent outcomes despite having reviewed similar facts.[79] Many courts consider factors such as control,[80] seeking out the image,[81] knowledge,[82] and deletion[83] without detailed explanations. This Part evaluates four factors, and their combined use, in turn.

1. Dominion and Control

Courts often consider what the defendant can actually do with the image, usually focusing on the user's ability to retain the image on the screen, enlarge it, zoom in or out, copy it, print it, and ultimately delete it. That is, courts focus on the user's level of control over the image.[84] This test is similar to the constructive possession test courts often apply in drug

78. *See infra* notes 80–83 and accompanying text.

79. *Compare* United States v. Romm, 455 F.3d 990, 1000–01 (9th Cir. 2006) (finding possession based on defendant's admission that he had some knowledge of the cache but with no indication that he actually had enough knowledge to access the cache), *with* United States v. Kuchinski, 469 F.3d 853, 862–63 (9th Cir. 2006) (finding no possession of images in cache where defendant argued that he had no knowledge whatsoever of the cache), *and with* State v. Jensen, 173 P.3d 1046, 1050, 1052–53 (Ariz. Ct. App. 2008) (finding that that there could be knowing receipt of images of child pornography regardless of whether the defendant "intended to save them or knew his computer was saving them").

80. *See, e.g.*, United States v. Tucker (*Tucker I*), 150 F. Supp. 2d 1263, 1266–67 (D. Utah 2001).

81. *See, e.g.*, Commonwealth v. Simone, No. 03-0986, 2003 WL 22994238, at *32 (Va. Cir. Ct. Nov. 12, 2003) ("The Court also observes that asking whether a defendant has reached out for and controlled the images recognizes and promotes the purpose behind the statute."); *see also* State v. Pickett, No. M2004-00732-CCA-R3-CD, 2005 WL 2438385, at *7 (Tenn. Crim. App. Oct. 3, 2005) ("[T]he printout demonstrates that the appellant repeatedly reached out for these websites in order to access the images . . . .").

82. *See, e.g.*, Commonwealth v. Gardner, 72 Va. Cir. 497, 498 (Va. Cir. Ct. 2007).

83. *See, e.g.*, United States v. Bass, 411 F.3d 1198, 1207 (10th Cir. 2005).

84. *See Romm*, 455 F.3d at 998 (noting the defendant's ability to keep the image on the screen, enlarge, copy, print, e-mail, and delete); *Tucker I*, 150 F. Supp. 2d at 1267 (noting defendant's ability to "*detain* [images] on his monitor as long as he liked," enlarge, manipulate, copy, zoom, show to others, and delete); Ward v. State, No. CR-05-1277, 2007 WL 1228169, at *3 (Ala. Crim. App. Apr. 27, 2007) (noting that defendant had the ability to copy, print, and e-mail); Commonwealth v. Diodoro, 932 A.2d 172, 174–75 (Pa. Super. Ct. 2007) (noting defendant's affirmative "actions of operating the computer mouse, locating the Web sites, opening the sites, displaying the images on his computer screen, and then closing the sites"). However, *Tucker I* seems to indicate that the ability to delete alone, without more, would still be sufficient to prove dominion and control. 150 F. Supp. 2d at 1266–67 (stating that "the ability to destroy is definitive evidence of control" after a lengthy discussion of various other factors that can indicate dominion and control); *see also supra* note 58 and accompanying text.

possession cases.[85] The test, therefore, represents an insightful application of traditional concepts to a new situation.

In *Tucker v. United States* (*Tucker I*),[86] the court explained that the defendant "could control [the images] in many ways:" He could copy them, print them, enlarge them and "zoom-in," show them to others, and copy them to other directories.[87] Based largely on evidence of control, the court found that the defendant possessed the images of child pornography on his computer.[88]

2. Seek and Obtain

Courts have also looked at the defendant's assertive steps that led to the viewing or downloading of child pornography images. The courts' use of this test often arises in cases involving cache files, when the defendant argues that he did not intend for the computer to download the file.[89] Indications of a user's actions to seek and obtain child pornography can include repeated visits to child pornography websites,[90] a defendant's subscription to child pornography websites,[91] and search terms related to child pornography.[92]

In *Commonwealth v. Simone*,[93] a search of defendant's computer revealed one image of child pornography that had been manually stored to the hard drive as well as a series of images that had been stored in the cache.[94] In analyzing "whether the defendant knowingly possessed the images found in the cache of his computer,"[95] the court emphasized the

---

85. *See* United States v. Tucker (*Tucker II*), 305 F.3d 1193, 1204 (10th Cir. 2002) (citing United States v. Simpson, 94 F.3d 1373, 1380 (10th Cir. 1996) ("defining 'knowing possession' in the drug context as encompassing situations in which an individual 'knowingly hold[s] the power and ability to exercise dominion and control' over the narcotics")); *see also* United States v. Riccardi, 258 F. Supp. 2d 1212, 1223 (D. Kan. 2003) ("The court believes that the government may prove knowing possession of child pornography, just as in the case of illegal possession of weapons, by establishing that a defendant constructively possessed the contraband.").

86. 150 F. Supp. 2d 1263 (D. Utah 2001).

87. *Id.* at 1267.

88. *Id.* at 1269.

89. *See id.* at 1268 ("The images would not have been saved to [the defendant's] cache file had [the defendant] not volitionally reached out for them."); *see also* State v. Pickett, No. M2004-00732-CCA-R3-CD, 2005 WL 2438385, at *7 (Tenn. Crim. App. Oct. 3, 2005) ("[A]ppellant repeatedly reached out for these websites in order to access the images that ended up being stored in his computer's temporary Internet file.").

90. *See Pickett*, 2005 WL 2438385, at *7.

91. *See* Fabiano v. Armstrong, 141 P.3d 907, 908 (Colo. Ct. App. 2006); *see also* Howard, *supra* note 67, at 1261.

92. *See* Howard, *supra* note 67, at 1261.

93. No. 03-0986, 2003 WL 22994238, at *1 (Va. Cir. Ct. Nov. 12, 2003).

94. *Id.* at *28–29.

95. *Id.* at *27.

defendant's actions to seek out images involving child pornography.[96] The court considered the search terms employed by the defendant, the defendant's possession of stories describing sexual acts by juveniles, and the possession of the image manually copied onto the hard drive, in finding that the "defendant reached out for these images with the intent to control and have dominion over them."[97]

3. Knowledge

Courts have applied knowledge as a factor in different ways. A common thread, however, is that any indication of knowledge by the defendant can be quite damning.[98]

In a remarkably short opinion, the court in *Commonwealth v. Gardner*[99] found that the defendant possessed child pornography based solely on a statement he made to investigators.[100] The court held that an inference of knowledge could fairly be drawn where the defendant said, "'I don't have too much' in response to a question [Investigator] DePena asked [the defendant] about the presence of child pornography on his computer."[101] The court explained that "it would seem that knowledge that a defendant had child pornography on his computer could be shown by the defendant's statements, his knowledge of the operational features of his computer, his general computer sophistication or other factors."[102]

4. Deletion

Courts often note a defendant's act to delete pornographic images. This factor often becomes significant as evidence of knowledge[103] or control.[104] In *United States v. Bass*,[105] the expert witnesses were unable to determine whether the numerous files of child pornography recovered from the defendant's computer had been automatically or manually saved.[106] The defendant argued that he merely viewed images on the Internet and was

---

96. *See id.* at *33.

97. *Id*.

98. *See* United States v. Kuchinski, 469 F.3d 853, 862–63 (9th Cir. 2006) (explaining that the conviction of the defendant in *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006), turned on the fact that the defendant knew that the cache would automatically copy the files).

99. 72 Va. Cir. 497 (Va. Cir. Ct. 2007).

100. *Id.* at 498.

101. *Id.*

102. *Id*.

103. *See infra* notes 105–11 and accompanying text.

104. *See infra* notes 148–49 and accompanying text.

105. 411 F.3d 1198 (10th Cir. 2005).

106. *Id.* at 1200.

ignorant of the computer's cache function.[107] The court found that the jury could have inferred the defendant's knowing possession from his use of certain software to delete the files from his computer.[108]

The dissent argued that the majority had rewritten the statute to criminalize mere viewing of child pornography.[109] First, the dissent argued that there was no evidence that the defendant knew that the images were being automatically saved to the computer.[110] Furthermore, the dissent pointed out the lack of evidence indicating control over the images.[111]

5. Combinations

Courts often employ more than one of the tests described above—especially when they seek to reconcile possession of computer images with the traditional definition of possession.[112] In *Ward v. State*,[113] the defendant viewed images of child pornography on his computer.[114] However, the defendant did not manually download the images onto his hard drive; all images found on his computers by the police were stored in the cache.[115] He argued that the statute specifically criminalized possession and not viewing,[116] and argued that he could not be guilty of possessing pornographic materials by merely viewing them on a computer screen.[117] The court specifically framed the issue as "whether an individual can be in possession of pornographic materials when he or she has viewed the pornographic materials on a computer screen but has not copied or saved those files to the computer."[118] After an in-depth study of case law dealing with a similar question,[119] the court explained that "the question becomes: Did the defendant specifically seek out the prohibited images and did he have the ability to exercise dominion and control over those images?"[120] The court's answer to the question was remarkably simple and coherent. First, the court found that the defendant reached out for the 288 images.[121]

---

107. *Id.* at 1201–02.
108. *Id.* at 1202.
109. *Id.* at 1206 (Kelly, J., dissenting).
110. *Id.* at 1207.
111. *Id.*
112. *See, e.g.*, United States v. Tucker (*Tucker I*), 150 F. Supp. 2d 1263, 1266–68, 1269 n.4 (D. Utah 2001).
113. No. CR-05-1277, 2007 WL 1228169 (Ala. Crim. App. Apr. 27, 2007).
114. *Id.* at *3.
115. *Id.* at *1.
116. *Id*. at *2.
117. *Id.*
118. *Id.* at *3.
119. *Id.* at *3–8.
120. *Id.* at *8.
121. *Id.*

Then, it found that the defendant had control over the images he was viewing because he could copy, print, e-mail, or send them to his home computer.[122] The court explained that the record did not reveal whether the defendant knew that the images would be saved to the cache[123] or whether the defendant *actually* controlled the images in the manner described.[124] However, the court found that the test made his knowledge as to these factors irrelevant.[125] Knowledge of the cache was not necessary to establish control or reaching out.[126] Control was established by demonstrating what defendant *could* do to the images, not what he actually did.[127]

B. *Courts' Approach to the Cache*

The courts' applications of the various factors hinge, at least in part, on the defense raised. In cases involving prosecutions of cached images, defendants advance two main arguments: (1) lack of knowledge regarding the cache function, and (2) lack of access to the cached files. In addressing these arguments, the courts have considered many of the same factors but have often come to differing conclusions. An analysis of the outcome of some of these cases reveals the source of the disparity: a limited understanding of the cache function. In the following analyses of *United States v. Tucker* (*Tucker II*),[128] and *United States v. Romm*,[129] two of the leading cases in the field, this Note seeks to expose this limitation.

1. *United States v. Tucker*

a. *Tucker I*

In *United States v. Tucker* (*Tucker I*),[130] the defendant accessed child pornography by participating in Internet newsgroups.[131] He paid a fee and received a password that enabled him to visit the websites on which he viewed child pornography.[132] When visiting the websites, the defendant

122. *Id.*
123. *Id.*
124. *Id*.
125. *Id*.
126. *Id*.
127. *Id*.
128. 305 F.3d 1193 (10th Cir. 2002); *see also* United States v. Tucker (*Tucker I*), 150 F. Supp. 2d 1263 (D. Utah 2001).
129. 455 F.3d 990 (9th Cir. 2006).
130. 150 F. Supp. 2d 1263 (D. Utah 2001).
131. *Id.* at 1265.
132. *Id*.

would view a series of thumbnails, which he could enlarge and view further.[133] The defendant explained that he did not download the images onto his computer because he could always access more images.[134] In fact, the defendant testified that he would often clear the cache after viewing images online, because he could access different images.[135] A forensic search of the defendant's computer revealed numerous images of child pornography on his hard drive.[136] However, all but one of the images were found on the cache.[137]

During the bench trial, Tucker argued that his viewing of child pornography did not amount to possession.[138] In its opinion, the district court set forth to resolve two issues: "1) whether Tucker had possession . . . and 2) whether such possession was knowing possession."[139] The court began by reviewing various definitions of possession, including natural possession[140] and constructive possession.[141] All the definitions cited by the court included an element of control.[142] Accordingly, the court began its analysis of whether defendant had possession by searching for indications of control in Tucker's viewing of the images.[143] The court explained that "[w]hile the images . . . were on his computer screen, he could control them in many ways: he could copy them . . . ; he could print them . . . ; he could enlarge them and 'zoom-in' . . . ; he could show them to other[s] . . . ; and he could copy them to other directories[.]"[144] The court, thus, found that "Tucker 'possessed' child pornography under the simple legal definition of the term."[145]

---

133. *Id*.

134. *Id*.

135. *Id.* The opinion does not say whether Tucker's deletion of the cache was intended to delete the images, so as not to have any images left on his computer or if he deleted them because he knew that he would access different images on his next online visit, making the images on the cache, whose purpose is to speed subsequent online viewing of the same image, useless. *See id.*

136. *Id.* at 1266.

137. *Id.*

138. *Id.* Tucker conceded to viewing child pornography but argued that "he never 'possessed' or 'knowingly possessed' any child pornography." *Id*.

139. *Id.*

140. "Black's Law Dictionary defines natural possession as '[t]he exercise of physical detention or control over a thing[.]" *Id.* at 1266–67 (alteration in original) (emphasis omitted) (quoting BLACK'S LAW DICTIONARY 1184 (7th ed. 1999)).

141. "'In order for an individual constructively to possess property, he must knowingly hold the power and ability to exercise dominion and control over it.'" *Id.* at 1267 (quoting United States v. Culpepper, 834 F.2d 879, 881 (10th Cir. 1987)).

142. *See id.* at 1266–67.

143. *Id*. at 1267.

144. *Id*.

145. *Id*. at 1268 n.4.

In rejecting Tucker's argument that the download to the cache was automatic and that he quickly deleted the effects of this process, the court asserted that the pictures were present only as a result of Tucker's volitional visits to the websites.[146] Furthermore, it interpreted Tucker's actions to delete the cache not as evidence that he did not wish to possess the images but rather as per se evidence of possession.[147] The court explained that "Tucker also demonstrated ultimate dominion and control over these images because he was able to destroy them" and that "the ability to destroy is definitive evidence of control."[148] In order to bolster its argument, the court likened the situation to drug possession, explaining that "[j]ust as a possessor of illegal narcotics is not able to escape criminal liability for possession by throwing drugs out a window, a person who possesses contraband such as child pornography cannot escape criminal liability by destroying it."[149] Finally, the court found the required element of knowledge demonstrated by Tucker's volitional reach for the images and by his constant deletion of the cache.[150]

b. *Tucker II*

On appeal from *Tucker I*, the Tenth Circuit largely agreed with the district court's analysis.[151] The Tenth Circuit noted expert testimony to the effect that the images on the cache are subject to the same control, such as copying and e-mailing, as any other data file.[152] In rejecting the defendant's argument that he did not voluntarily cache the files and that he deleted them as soon as possible, the court stated: "Since he knew his browser cached the image files, each time he intentionally sought out and viewed child pornography with his Web browser he knowingly acquired and possessed the images."[153] Thus, the court, found that Tucker possessed the images in his cache.[154]

c. Analysis of *Tucker I* and *Tucker II*: Did the Courts Get It Right?

The district court's application of the simple legal definition of possession in *Tucker I* demonstrates how possession of a digital image can be analyzed similarly to possession of a physical object. The *Tucker I*

146. *Id*. at 1268.

147. *See id*.

148. *Id*. at 1267. The court found that "[l]ogically, one cannot destroy what one does not possess and control." *Id.*

149. *Id.* at 1268.

150. *Id*. at 1269.

151. United States v. Tucker (*Tucker II*), 305 F.3d 1193, 1204–05 (10th Cir. 2002).

152. *Id*.

153. *Id*. at 1205.

154. *Id*.

court pointed out a series of activities, such as choosing to retain the image, copying, and zooming, that would establish control in any situation.[155] Arguably, the *Tucker I* court already set forth enough factors in its control analysis to find that Tucker controlled and thus possessed, the images that he had viewed on his monitor.[156] In fact, the court itself explained that it found possession "under the simple legal definition" of possession.[157] However, the court continued with a strained effort to reconcile the automatic download of the images to the cache with its previous control analysis.[158]

The district court's explanation of control over the cache seems wanting despite this point receiving the most attention in the court's analysis. The district court essentially offered the same proposition, arguably with the same flaw, various times. In *Tucker II*, the court of appeals restated the same reasoning. The two courts found dispositive the fact that "[t]he images would not have been saved to his cache file had Tucker not volitionally reached out for them."[159]The courts did not consider at all how the programming of the computer works to store the information to the cache automatically. However, if the computer were not programmed to automatically save Internet images, Tucker could have viewed and manipulated the images while on the Internet without causing a file to download onto his hard drive. Obviously, Tucker would have always had the option to manually download the file, but he would have had to make a conscious decision to initiate the download. Therefore, under the analysis applied by the courts, Tucker, with enough knowledge of the law or programming, could have avoided conviction by simply ignoring the fact that his computer's cache existed.

Furthermore, the *Tucker I* court's reliance on destruction as dispositive evidence of control, and thus possession, over the images in the cache, is plagued with similar shortcomings. The opinion does not indicate that Tucker knew enough about computers to override the system warnings and actually access the images on the cache. In fact, the *Tucker I* court's control analysis expressly indicated that Tucker controlled the images "[w]hile the images . . . were on his computer screen."[160] The only indication of Tucker's control over the cache is his manual deletion of the cache, which, as previously explained, is a fairly simple task that can be accomplished by a computer user without any knowledge of how to access

155. *Tucker I*, 150 F. Supp. 2d at 1267.
156. *See supra* text accompanying note 144.
157. *See supra* text accompanying note 145.
158. *Tucker I*, 150 F. Supp. 2d at 1266–68.
159. *Tucker II*, 305 F.3d at 1199 (citing *Tucker I*, 150 F. Supp. 2d at 1268).
160. *Tucker I*, 150 F. Supp. 2d at 1267.

the information that is actually inside the cache.[161] Therefore, the court's conclusion that deletion is definitive evidence of control as—"one cannot destroy what one does not possess"[162]— is flawed. As pointed out by Assistant District Attorney Ty E. Howard,[163] "[t]hat logic falls short," since ability to destroy does not necessarily show possession.[164] For example, every driver on the road has the ability to destroy any scooter, mailbox, fence or other car in sight by crashing into it.[165] However, no one would say that, as a result, every car driver possesses every scooter, mailbox, fence, and other car in sight. Alternatively, consider an individual who borrows a coat from a friend and, later that night, while in the restroom, notices a small bag of drugs in the pocket. She flushes it down the toilet immediately. The fact that she destroyed it does not prove that she possessed the drugs, within the legal definition. The court's own words, however, reveal that it reached the opposite conclusion regarding deletion.[166] In its proposed comparison to a drug transaction, the court explains that one cannot get rid of one's possession over an item by destroying the item.[167] Therefore, the court's analysis necessarily presumes that the item is already possessed; that is, there would be no need to get rid of the possession if there was no possession initially. This leads to the question of how the presumed possession arose. The court's analysis never ascertains how it is that Tucker possessed the images on the cache *before* he deleted them.

The circuit court's analysis is more complete because the court at least includes expert testimony regarding the user's ability to control images in the cache.[168] Arguably, the ability to manipulate these images establishes the control necessary to constitute possession. However, there is still no indication that Tucker had the computer skills necessary to exercise control over the images in the cache. The end result is that the circuit court in *Tucker II* comes closer than the district court to hitting the mark, but it is still missing a link in the evidentiary chain.

2. *United States v. Romm*

In *United States v. Romm*,[169] the defendant admitted viewing images of child pornography on his computer but argued that "he [could not] be

161. *See supra* note 75 and accompanying text.
162. *Tucker I*, 150 F. Supp. 2d at 1267.
163. Howard, *supra* note 67, at 1227 & n.†.
164. *Id.* at 1258.
165. *See id.*
166. *See supra* text accompanying note 149.
167. *Id*.
168. *See supra* text accompanying note 152.
169. 455 F.3d 990 (9th Cir. 2006).

found guilty of possessing . . . child pornography, when he merely viewed child pornography without 'downloading' any of it to his hard drive."[170] In viewing the files online, Romm previewed a series of thumbnails and enlarged those he wanted.[171] The facts set forth by the court indicate that, in his conversations with the police officers who arrested him, Romm used the terms "save" and "download" to describe his actions.[172] Expert witnesses for the government testified that all child pornography files had been deleted from the computer but that images once existed on the hard drive of the computer.[173] The opinion suggests that some images might have been originally stored outside the cache,[174] but the portions of the expert testimony included in the opinion do not contain this express finding.[175] The expert witnesses for both sides explained that images stored on the cache are "accessible, albeit 'system-protected,'"[176] revealing that at least some special knowledge (the location of the cache) is required to access them.[177] Finally, none of the expert witnesses concluded that Romm had actually accessed the cache on his computer.[178]

The Ninth Circuit held that there was sufficient evidence of control to find that Romm possessed the images "in his cache."[179] In its analysis, the court first found that a user can access an image in the cache.[180] Furthermore, the court found that the files in the cache could be converted into visual images and thus fell within the § 2252A definition of "visual depiction."[181] The court found that Romm "exercised control over the cached images while they were contemporaneously saved to his cache and displayed on his screen."[182] The court distinguished Romm's control over the images from the saving of images to the cache that occurs when an

170. *Id.* at 993–94 (footnote call number omitted).

171. *Id.* at 993.

172. *Id.* at 995.

173. *Id.*

174. *See id.* at 995 ("Luckie confirmed that all of the child pornography on Romm's computer had been deleted. The vast majority of the images Luckie found had been deleted from Romm's internet cache.").

175. *Id.* at 994–96, 997–1001.

176. *Id*. at 995.

177. *Id.* at 995–96.

178. *See id.* Luckie, an expert witness for the Government, testified that Romm either deleted cache manually by accessing the cache and deleting the files or used the Internet browser to delete the cache. *Id.* at 995. Romm's expert found no evidence that Romm had ever gone into the cache. *Id.* at 996.

179. *Id.* at 998.

180. *Id.*

181. *Id.* at 998–99; *see also* 18 U.S.C. § 2256(2)(B)(5) (2006) ("'[V]isual depiction' includes . . . data stored on computer disk or by electronic means which is capable of conversion into a visual image[.]").

182. *Romm*, 455 F.3d at 1000.

individual accidentally views a pop-up. The court explained that Romm's intentional searching and viewing of images, rather than an accidental pop-up, resulted in the images that were saved in the cache.[183] The court stressed the coincidence of Romm's control over the image on the screen and the download to the cache and found that "Romm had access to, and control over, the images that were displayed on his screen and saved to his cache."[184]

The circuit court found control, and thus possession, over the image on the screen but convicted Romm of possession of—not that image—but the copy of that image in (the cached image). The reason behind this bizarre outcome is that Romm's control over the image on the screen occurred at the same time that cached image was created.[185] A hypothetical may help illustrate the difference:

Let us assume that Linda has bought the latest high definition DVD player to watch movies in her home. The DVD player was actually developed by a computer genius (Gino) whose goal is to have a copy of every movie ever created. For such purposes, Gino has programmed the hundreds of DVD players that he plans to sell with a mechanism that copies movies as they are being watched with the DVD player. The copy is saved to a "superchip" that is hidden in the underside of the DVD player. The superchip continues to automatically store movies until it is full, at which time it erases itself. Alternatively, the superchip's contents are deleted if the user resets the DVD player for any reason. The owners of the DVD players do not know about the superchip and have no way to access the superchip. Gino has offered free maintenance of the DVD players in hopes that buyers will call him to their houses so that he can use his personal supercomputer to get the movies from the superchip. Once Gino accesses the superchip, he can play the movies stored inside just like any other movie.

The point of the hypothetical is to illustrate the difference between the movie that Linda is viewing on her screen and the movie that goes into the superchip. Linda can control the movie on her television screen by pausing it, re-starting it, fast-forwarding, re-winding it, and even removing it from her television screen by removing the DVD from the DVD player. Ignoring the physical disk on which the movie is recorded, it can be said that Linda possesses the movie on her screen because her ability to re-wind it, restart it, or remove it gives her dominion and control over the movie on the screen. However, Linda cannot assert her control over the copy of the movie stored on the superchip. The copy of the movie in the superchip, despite being identical to the movie that Linda is watching on her screen,

183. *Id.*
184. *Id.* at 1000–01.
185. *See id.* at 998–99.

is a completely different "object" from the movie on the screen.[186] The mere fact that the copy on the superchip was created at the same time that Linda had control over the movie on the screen does not give her any more control over the movie on the superchip than if the copy were created at some other time.

Merging the analogy into the *Romm* court's holding, the court would find that Romm "exercised control over the [movies in the superchip] while they were contemporaneously saved to [the superchip] and displayed on his [TV] screen."[187] No case law supports the court's finding. Establishing control over the independent copy requires an independent analysis of the ability to control *that* item. Although a computer user with enough knowledge could access the images in the cache, expert witness testimony included by the *Romm* court in the opinion reveals no evidence that Romm ever accessed the images in the cache.[188] The only apparent indication of control over the cache was the deletion of the images in the cache, which can occur for any number of reasons.[189] In fact, the expert witnesses were also unable to pinpoint whether the images on the cache were deleted automatically because the cache was full, deleted by the user using the browser—a fairly simple procedure that can be done by the average computer user—or manually deleted from the cache.[190] Therefore, the court in its opinion relied on insufficient evidence to establish control over the images in the cache of Romm's computer. Thus, there was insufficient evidence to establish possession over the images located in Romm's cache.

V. PROPOSED UNIFORM SOLUTION

A. *The Underlying Framework*

It is an easy stretch to extend the intuitive idea of possession to include an image that a user has actively downloaded onto his hard drive. However, it might not be as easy to extend that idea to an image inside a cache file, which the user did not intentionally place there and most likely cannot access.[191] The courts' reluctance to find possession where it is apparent that defendants had no knowledge about the cache is

186. *Cf. supra* note 66 and accompanying text (discussing the mechanisms by which the cache creates a different file from that which is represented on the screen).

187. *See supra* text accompanying note 182.

188. *See supra* notes 175–78 and accompanying text.

189. *See supra* note 75 and accompanying text (discussing deleting the cache).

190. *See supra* notes 175–78 and accompanying text.

191. *See supra* note 72 and accompanying text.

understandable.[192] However, it also seems unreasonable that a person that willingly accessed, viewed, and arguably controlled images of child pornography would not be convicted as a result of his ignorance regarding the workings of computer cache.

This situation is problematic for three reasons. First, it encourages willful blindness.[193] Second, it would result in disparate treatment between those choosing to download images from a website and those with enough legal knowledge to understand that they should view the images without downloading them, even though both have the same control over the image while it is on their screen.[194] Finally, courts' holdings become even more contradictory because many of those who know about a computer's cache are unlikely to be able to access it.[195]

---

192. *See, e.g.*, United States v. Kuchinski, 469 F.3d 853, 863 (9th Cir. 2006) ("Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images. To do so turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control.").

193. Alternatively, it encourages evasive planning and deceit by child pornography viewers. Taking their cue from the case law inferring knowledge of the cache from simple tasks such as clearing it, users could learn not to cover their tracks at all in efforts to fool courts into thinking that they have no knowledge of the cache. *See* United States v. Bass, 411 F.3d 1198, 1202 (10th Cir. 2005) (finding sufficient evidence of knowledge of the cache where defendant used two programs in attempts to remove child pornography from his computer so that his mother would not find it).

194. *Compare supra* Part III.B (discussing downloading), *with supra* Part III.C (explaining viewing without downloading and the effect of cache memory).

195. *See supra* Part III.C. The courts seem to ignore the third kind of user, the one that falls between the person that has no idea about cache and the person that knows about it but does not have full access to it. The latter knows about cache and how it works but does not know how to access the images inside it. *See id.* This third person has no more access to the images in the cache than the first person who has no idea that cache exists. However, this individual tends to be viewed by courts as no different from the person that has full access to the cache. *See supra* Part IV.B.1; *see also Bass*, 411 F.3d at 1202. An example helps demonstrate the difference in the three situations:

Three Buyers seek out their usual dealer and purchase some marijuana, which they consume immediately. The dealer is competing with another dealer and has decided to give his customers a surprise bonus for the rest of the week. After the transaction, the dealer rides his bike to each of the three customers' houses and throws a bag of marijuana through each of their bathroom windows. Buyer 1 knows nothing about the promotion. His bathroom door is broken and he is using another bathroom, so Buyer 1 never finds the promotional bag. Buyer 2 had bought from the dealer this week and knows about the promotion, but his bathroom door is also broken. He has no access to the bathroom. Buyer 3 knows about the promotion, and has full access to his bathroom. As a final note, the dealer happens to be a very determined person who would have thrown the promotional bags in the windows even if the three Buyers were not interested in receiving them. In fact, Buyer 2 would very much prefer that the dealer did not drop anything off at his house, and, if he had access to the bathroom, he would close the window in order to prevent the delivery from occurring. After the delivery, Buyer 2 inserts a thin pole through his window, which he uses to push the bonus bag into the toilet (he cannot actually bring it out the window), and flushes it. His

As unearthed by Ty E. Howard, a large part of the problem underlying the confusion in this area of the law is the fact that courts do not tend to recognize the existence of two distinct possible approaches to possession of a digital image. Under the first approach—the "evidence of possession approach"—images stored in the cache are accepted as evidence of prior possession. Under the second approach—the "present possession approach"—the images in the cache are the objects actually being possessed.[196] Under the "evidence of possession approach," the defendant is charged with possession of the image that was once on the screen,[197] whereas under the "present possession approach" the defendant is charged with possession of the cached file itself.[198]

1. Present Possession Approach

The two approaches lead to two very different kinds of cases that are open to different legal arguments and different evidence. In the "present possession approach," the defendant is prosecuted for possessing whatever files are presently in the computer, be they cached files or manually saved files.[199] A case within this framework will revolve around the element of knowledge. Proving knowing possession of manually saved files is not difficult because the process of manually saving the file demonstrates that control is apparent to the user.[200] However, knowledge becomes a primary

---

neighbor sees him and calls the police.

So far, most would agree that Buyer 3 possesses the bonus bag and Buyer 1 does not possess the bonus bag. But what about Buyer 2? The only difference between Buyer 1 and Buyer 2 is that Buyer 2 happens to know that the promotion exists. It seems unreasonable that Buyer 2 would be liable for taking steps to destroy something that he never wanted and never had access to, but Buyer 1 is not liable at all because Buyer 1 did nothing. Furthermore, it would also likely be a difficult task to demonstrate that Buyer 2 did have knowledge of the promotion if he had chosen to do nothing about the drugs in his bathroom.

Similarly, in the context of possession of images in the cache, it is difficult to demonstrate that a defendant has knowledge of the workings of the cache. Both the *Tucker* and *Romm* courts seem to be looking for something beyond just "some knowledge" of the cache's existence. However, the outcomes of the two cases allow an argument that the user need not have access to the cache before he possesses the images in them.

196. Howard, *supra* note 67, at 1254. *Cf.* State v. Jensen, 173 P.3d 1046, 1051, 1052–53 (Ariz. Ct. App. 2008) (focusing on the use of the screen and distinguishing *Romm* and *Tucker*, among other precedent and finding that there could be knowing receipt of images of child pornography regardless of whether the defendant "intended to save them or knew his computer was saving them").

197. Howard, *supra* note 67, at 1255.

198. *Id.* at 1254–55.

199. *Id.*

200. *See* United States v. Riccardi, 258 F. Supp. 2d 1212, 1224 (D. Kan. 2003) ("This evidence [of saving images onto the computer] suggests that Mr. Riccardi took affirmative steps to preserve the child pornography on his computer and, therefore, knowingly possessed such

issue where the defendant has not manually downloaded the images and is being prosecuted for possessing the images in the cache.[201] Defendants being prosecuted for possessing images in the cache often contend that they did not know that the images were downloaded to the cache[202] or, alternatively, that they did not want the images to be downloaded to the cache.[203] Since the argument concerns the defendant's state of mind, it is not difficult for him to make, and the prosecution's evidence to the contrary is often circumstantial.[204] As a result, the evidence presented involves expert testimony regarding the source of the images and the process through which images are downloaded to the cache.[205] Furthermore, since many courts rely on indicia of control in finding possession, a battle of the experts arises, where experts on both sides indicate that the cache is located in a system-protected area of the computer and express their opinions as to whether the defendant ever manually accessed the cache.[206] Case law reveals that establishing knowing possession of the cache can be a daunting task that can lead to questionable outcomes.[207] Finally, this approach rewards informed offenders by effectively immunizing individuals who have enough legal knowledge to avoid manually downloading files and enough computer skill to fully disable the cache function and browser memory.

2. Evidence of Possession Approach

In the "evidence of possession approach," the defendant is prosecuted for possessing the image that was once on the screen.[208] This approach can be attacked because many possession statutes do not speak to viewing and some will argue that mere viewing does not constitute possession.[209]

---

items . . . .").

201. Defendants often defend by arguing a lack of knowledge of the cache. *See* United States v. Kuchinski, 469 F.3d 853, 862 (9th Cir. 2006); United States v. Bass, 411 F.3d 1198, 1202 (10th Cir. 2005).

202. Howard, *supra* note 67, at 1257.

203. *See* United States v. Tucker (*Tucker I*), 150 F. Supp. 2d 1263, 1268 (D. Utah 2001) (responding to defendant's arguments that defendant did not cause the images to be downloaded onto the cache and that defendant immediately deleted them when he logged off the Internet).

204. *See Bass*, 411 F.3d at 1202 (interpreting the defendant's use of programs to delete child pornography files from his computer as evidence of knowledge).

205. *See, e.g.*, United States v. Romm, 455 F.3d 990, 995 (9th Cir. 2006).

206. *See* United States v. Tucker (*Tucker II*), 305 F.3d 1193, 1204–05 (10th Cir. 2002).

207. *See supra* Part IV.B.2.

208. *See* Howard, *supra* note 67, at 1254–55.

209. For examples of courts indicating that passive viewing does not constitute possession, see *United States v. Stulock*, 308 F.3d 922, 925 (8th Cir. 2002), which quoted without disapproval the district court's finding "that one cannot be guilty of possession for simply having viewed an image on a web site." *See also* United States v. Perez, 247 F. Supp. 2d 459, 484 n.12 (S.D.N.Y. 2003); Strouse v. State, 932 So. 2d 326, 328 n.3 (Fla. 4th DCA 2006). For examples of defendants

However, these arguments can be defeated with proof that the user controlled the images on the screen.[210] Evidence of control can establish that the defendant was not a passive viewer.[211] Furthermore, since the user can easily see the image on the screen, the user cannot argue a lack of knowledge of his possession over the image. Therefore, under this approach, the application of the law to the facts becomes simpler.

It is not uncommon to find courts straddling the line between the "present possession" and "evidence of possession" approaches.[212] A failure to understand the difference between the two approaches can lead to confusing outcomes.[213] A functional definition of what constitutes possession of child pornography, as a threshold matter, requires a choice between these two approaches. The ability to limit uncertainty surrounding the element of knowledge makes the "evidence of possession" approach considerably easier to apply.[214] The use of this approach would limit the complicated arguments about the workings of the cache. Defendants would no longer be able to plead ignorance of how the computer works because they would be being prosecuted for possessing an item that they could clearly see on the screen. The court would then be free to focus on factors more closely related to traditional determinations of possession.

It is likely that courts might, as a matter of policy, be concerned about an approach that finds possession in the mere viewing of an image. However, the choice set forth by Ty E. Howard's framework is just the first step in the analytical process.[215] As applied in this Note, the purpose of the framework is not to actually test for possession of child pornography but to guide the court in its examination of the evidence that will establish possession of child pornography.

B. *Proposed Test*

1. Explanation of Proposed Test

There are many ways to access child pornography through the Internet. Although most of them require a user's active participation, it is possible

---

arguing that mere viewing does not constitute possession, see *supra* note 64 and accompanying text.

210. *See* United States v. Tucker (*Tucker I*), 150 F. Supp. 2d 1263, 1267 (D. Utah 2001); *see also* State v. Jensen, 173 P.3d 1046, 1050, 1052 (Ariz. Ct. App. 2008) ("Contrary to [the defendant]'s contention, the act of intentionally searching for and accessing a website for child pornography is not the equivalent of merely looking at a picture in a museum.").

211. *Jensen*, 173 P.3d at 1050, 1052.

212. *See supra* note 196 and accompanying text.

213. *See, e.g.*, *supra* Part IV.B.2.

214. *See* Howard, *supra* note 67, at 1253–64 (discussing further the application of the two frameworks in diverse situations).

215. *See id.*

to encounter child pornography unintentionally.[216] An adopted test should therefore cast a net narrow enough to exclude an accidental viewer, no matter how much adult pornography the person chooses to view but wide enough to catch all those who actually desire to find child pornography. Furthermore, the test should take into account the pattern displayed by case law, where willing viewers defend themselves by proving a lack of computer sophistication and should seek to avoid rewarding the feigned ignorance of defendants.

So far, courts have been generally unsuccessful at developing a test that can be applied uniformly to all the situations above, and academic commentary on the subject is scarce.[217] However, after making the choice to view cache as evidence of possession, the task of choosing a test that will work in all situations becomes manageable.

This Note proposes a test that combines the often considered "dominion and control" and "seek to obtain" factors into a two-part test. This combination would allow the courts to include all willing viewers of child pornography in its net while excluding all accidental recipients. First, the dominion and control portion of the test allows possession of electronic child pornography to align with the courts' traditional definition of possession.[218] The approach calls for a concentration on indications of viewer control such as the user's ability to view for as long as he wants, and the ability to enlarge, zoom, copy, download, share, print, edit, and close the image on the screen. These activities readily compare with activities that a person handling a paper copy of child pornography in a magazine could engage in: the person can look at each image for as long as he wants, unfold a larger center-fold if one is available, use a magnifying glass to look at the image in more detail, make a copy using a photocopy machine, show it to a friend, make a copy for a friend to take home with them, and choose to destroy the whole magazine or simply put it away.

In the second part of the test, the "seek to obtain" portion serves the dual purpose of: (1) ensuring that only those individuals who specifically sought out child pornography, as opposed to those searching for adult pornography, are convicted, and (2) allowing the prosecution of those who did not intend to find child pornography but sought to keep it once they found it. The test would operate much as it has before, allowing courts to

---

216. GAO REPORT, *supra* note 47, at 2.

217. Howard, *supra* note 67, at 1249. Academic commentary has largely concentrated on the area of virtual child pornography. *See* Jason Baruch, Comment, *Constitutional Law: Permitting Virtual Child Pornography—A First Amendment Requirement, Bad Policy, or Both?*, 55 FLA. L. REV. 1073 (2003).

218. *See supra* notes 13, 141–43 and accompanying text.

look at the search terms used by the defendant,[219] the websites to which the defendant subscribes,[220] and the number of images of child pornography found on the defendant's computer as evidence of a defendant's intent to seek out images of child pornography specifically.[221] The knowledge element of the statute would thus be satisfied,[222] and the purpose behind the statute would be promoted.[223] The user's specific choices would be strong evidence indicating whether or not the user searched for child pornography, and therefore evidence of the user's knowledge of the images being downloaded.[224] Since courts and experts have often stated that the terms employed to search for child pornography are specific and, consequently, distinguishable from the terms used to search for adult pornography,[225] individuals searching strictly for adult pornography would, under this prong of the test, be able to demonstrate that they were not seeking child pornography.

The test does not embody a set number of child-pornography related search terms or images that would be dispositive about whether the defendant sought out child pornography. These specified indicators, as well as any others not included here, are proposed as circumstantial

---

219. *See* United States v. Carani, 492 F.3d 867, 871 (7th Cir. 2007).

220. *See supra* text accompanying note 77; *see also* United States v. Tucker (*Tucker I*), 150 F. Supp. 2d 1263, 1265 (D. Utah 2001).

221. Although generally not conclusive, the number of images of child pornography found on the defendant's drive often make up part of a court's finding. Howard, *supra* note 67, at 1263 n.183; *see, e.g.*, United States v. Romm, 455 F.3d 990, 993 (9th Cir. 2006) (counting forty-two images); Ward v. State, No. CR-05-1277, 2007 WL 1228169, at *1 (Ala. Crim. App. Apr. 27, 2007) (counting 288 images); Commonwealth v. Simone, No. 03-0986, 2003 WL 22994238, at *28 (Va. Cir. Ct. Nov. 12, 2003) (counting 260 images). A large number of child pornography images in proportion to the total number of adult pornographic images also found on a computer would be evidence weighing against a defendant's arguments that child pornography was accidentally found while searching for adult pornography.

222. *See supra* notes 66–70 and accompanying text (emphasizing the knowledge requirement in the statutes).

223. *See* cases cited *supra* note 81.

224. In *United States v. Carani*, the defendant contended that any child pornography images found on his computer had been downloaded inadvertently while searching for adult pornography, and he argued that he was not knowledgeable about computers. 492 F.3d at 870–71. However, a search of the hard drive by law enforcement revealed more than 5,000 images of child pornography. *Id.* at 871. "[Law enforcement agents] concluded that Carani was actively seeking out child pornography, as a home computer would not otherwise contain so many references to terms associated with child pornography[,]" and testified at trial that "[the child pornography] videos were not downloaded in large chunks along with adult pornography; rather, they were downloaded along with other child pornography, in groups of five or six." *Id.* The jury found the defendant guilty of possession of child pornography. *Id.* at 872. The Seventh Circuit held that "[t]he government presented evidence sufficient for the jury to infer that Carani suspected that files he was downloading and sharing with others contained child pornography[.]" *Id.* at 874.

225. *See supra* text accompanying notes 45–46.

evidence[226] of the defendant's actions to seek out child pornography. For example, consider the case of a defendant who is arguing that he only intended to obtain adult pornography but sometimes found child pornography, where expert testimony indicates the presence of 500 images of child pornography and 500 images of adult pornography in the computer.[227] In such a case, the predominance of child pornography images—fifty percent of the total—would be circumstantial evidence of the defendant's actions to seek out both adult pornography and child pornography specifically because it is highly unlikely that searches for adult pornography would return child pornography images fifty percent of the time.

At the same time the "seek-to-obtain" prong will also address the situation where an individual accidentally views or receives child pornography but then, instead of destroying it, seeks to keep it. This reasoning is expressed in *Commonwealth v. Simone*,[228] which explained:

> By analogy, one might consider the following hypothetical. If a person walks down the street and notices an item (such as child pornography or an illegal narcotic) whose possession is prohibited, has that person committed a criminal offense if they look at the item for a sufficient amount of time to know what it is and then walks away? The obvious answer seems to be "no." However, if the person looks at the item long enough to know what it is, then reaches out and picks it up, holding and viewing it and taking it with them to their home, that person has moved from merely viewing the item to knowingly possessing the item by reaching out for it and controlling it. In the same way, the defendant in this case reached out for prohibited items and, in essence, took them home.[229]

A person who accidentally comes across child pornography has a choice between getting rid of it or keeping it. The person who makes the choice of immediately getting rid of the child pornography by destroying it or throwing it away never sought to possess. This person "has not formed the requisite knowledge, and is lacking the necessary mens rea."[230] However, an individual who accidentally finds child pornography and

---

226. *Cf.* State v. Jensen, 173 P.3d 1046, 1050, 1052 (Ariz. Ct. App. 2008) (discussing how knowledge may be inferred from circumstantial evidence and stating that "internet searches for this kind of material is evidence that the computer operator knew what he was going to and did receive").

227. *See supra* note 224 and accompanying text.

228. No. 03-0986, 2003 WL 22994238 (Va. Cir. Ct. Nov. 12, 2003).

229. *Id.* at *33.

230. *Jensen*, 173 P.3d at 1052.

decides to retain it has, at the point in which they decide to keep it, reached out for the image of child pornography.[231] This analysis is useful in an e-mail situation where the defendant does not solicit the child pornography. His conscious decision to keep the e-mail would establish possession, whereas a decision to quickly delete would establish the opposite.

2. Application of the Proposed Test to Existing Case Law

The joint application of these two factors can lead to a cohesive analysis.[232] The application of the entire framework proposed in this Note would also have resulted in stronger opinions in both *Tucker* and *Romm*.

First, a large part of the complication that the *Tucker* courts faced would be resolved by taking the evidence of possession approach. Both the appellate and the district courts spent a great deal of time trying to establish control over the images in the cache. Under the proposed test, that analysis would become superfluous once it was established that the defendant had control over the image on the screen. As evidenced by *Tucker I*, there was ample evidence of the defendant's control over the images on the screen. The next step would be to establish that the defendant sought out the images. The courts could have looked at the evidence regarding what searches the defendant ran and at the prominence of child pornography relative to other types of files on his computer as evidence that the defendant affirmatively sought out child pornography. In this way, the court could have proven knowing constructive possession with a simpler analysis than either court employed. Furthermore, the questionable assertions regarding deletion as per se evidence of control would become unnecessary, leading to a stronger opinion.

Similarly, the courts could have established possession in *Romm* without resorting to the argument that the defendant controlled the images that were created in the cache while Romm controlled the images on the screen. In fact, if both the *Tucker* and *Romm* courts had applied this proposed test, the opinions could sound remarkably similar. Romm's control would be proven by his ability to manipulate the images while they were on his screen, and his seeking out of the images could be demonstrated with expert testimony of the search terms he used. These opinions would thus reinforce each other, creating strong precedent for what constitutes possession of electronic child pornography.

---

231. *Id.* at 1049–50 ("[T]hat same person could be in possession of the unlawful image if it is retained.").

232. *See supra* text accompanying notes 113–27.

VI. CONCLUSION

Bans on possession of child pornography seek to protect children who are irreparably harmed in its production. Possession of child pornography is not by nature an Internet crime;[233] however, the Internet's speed, ease of use, and offer of anonymity have made the web a convenient way to access child pornography.[234] It can be expected that the Internet will continue to dominate as the most common medium to access child pornography.

The law has struggled to keep pace with technology in this field. In establishing whether there is possession of digital data, many courts have relied on internal computer processes that the user cannot see. The result has been complication and inconsistency. Under current case law, an avid consumer of child pornography whose computer contains evidence of thousands of images of child pornography, would, if prosecuted in the Ninth Circuit, not be held liable if he argues that he did not know about his computer's cache.[235] In contrast, the same avid consumer would be held liable if prosecuted in Arizona state court.[236]

As proposed in this Note, a test that may be applied to any digital possession scenario would lead to more uniform outcomes. A focus on the user's search and the user's ability to control and manipulate the image displayed on the screen would enable the courts to concentrate on what the user can see on the screen rather than concentrating on internal processes that the user does not see. The requisite proof under such a test is clear: The prosecution must establish that the user sought out child pornography and, once found, the user could manipulate and control the images. The user's degree of computer sophistication—beyond the ability to search and control images off websites—becomes irrelevant. The result is more certainty and predictability because outcomes would no longer vary according to each user's computer sophistication. Furthermore, concentrating on the volitional consumption of child pornography is consistent with the interest of protecting the young victims of child pornography.[237]

---

233. Child pornography has been available through other mediums since before the advent of the Internet in the early 1990s. *See, e.g.*, Jacobson v. United States, 503 U.S. 540, 547 (1992) (prosecution for mail receipt of magazines containing child pornography); United States v. Driscoll, No. 94-3591, 1995 WL 368839, at *2 (7th Cir. June 20, 1995) (prosecution for possession and transportation of child pornography in VHS form).

234. GAO REPORT, *supra* note 47, at 1 ("In recent years, child pornography has become increasingly available as it has migrated . . . to the World Wide Web. As you know, a great strength of the Internet is that it includes a wide range of search and retrieval technologies that make finding information fast and easy.").

235. *See supra* text accompanying notes 2–8.

236. *See supra* note 79 and accompanying text.

237. *See supra* text accompanying note 52.